REMARKS

This communication is a full and timely response to the aforementioned Office Action dated December 11, 2008 and the Advisory Action dated May 30, 2008. By this communication, claims 1, 7, 17 and 25 are amended, and claims 13, 15, 16 and 21 are cancelled. Claims 2-6, 8-12, 18-20, 22-24, 26 and 27 are not amended and remain in the application. Thus, claims 1-12, 17-20 and 22-27 are pending in the application. Claims 1, 7, 17 and 25 are independent.

Reconsideration of the application and withdrawal of the rejections of the claims are respectfully requested in view of the foregoing amendments and the following remarks.

I. Rejections Under 35 U.S.C. § 102(e)

Claims 13 and 16 were rejected under 35 U.S.C. § 102(e) as being unpatentable over Smetters et al. (U.S. Patent Application Publication No. 2004/0088548, hereinafter "Smetters"). This rejection is believed to be moot in view of the cancellation of claims 13 and 16.

II. Rejections Under 35 U.S.C. § 103(a)

A. Claims 1, 4, 5, 7, 8, 10, 12, 17 and 20-25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Smetters in view of Benson (U.S. Patent No. 6,047,242).

To establish a *prima facie* case of obviousness, the applied references must disclose or suggest all the claim limitations. See MPEP 2142; 706.02(j). If the applied references fail to disclose or suggest one or more of the features of a claimed invention, then the rejection is improper and must be withdrawn.

Without acquiescing to this rejection, independent claims 1, 7, 17 and 25 have each been amended to emphasize distinctions between the claimed invention and the applied references. Accordingly, Applicant respectfully submits that the claimed invention is patentable over the applied references for the following reasons.

An exemplary embodiment of the present invention provides a communication system in which a device 100 and a client 200 communicate with each other through a network 300 (see Figure 1).

As shown in Figure 2, for example, the device 100 comprises a first storage device 118 which stores a root certificate 126. The root certificate 126 includes a public key paired with a private key and is signed with the private key. The device 100 also comprises a certificate creator 124 which creates a second certificate 128, when a connection for communication is requested by the client 200. The second certificate 128 designates the root certificate 126 as a certificate authority at a higher level and is signed with the private key included in the root certificate 126 (see, for example, line 25 on page 12 to line 2 on page 13 of the specification). The device 100 comprises a communication device 106 which transmits the second certificate 128 created by the certificate creator 124 to the client 200 (see Figure 2).

The client 200 comprises a second storage device 214 which has stored therein, before the connection for communication is requested to the device 100, the root certificate 222 (126) stored in the first storage device 118 of the device 100 (see Figure 3). The client 200 also comprises a verifier which verifies the signature of the second certificate 128 received from the device 100 with the root certificate 222 (126) stored in the second storage device 214.

Accordingly, the disclosed embodiment provides that the root certificate 222 (126) stored in the first storage device 118 of the device 100 is also stored in the second storage device 214 of the client 200 before the client 200 requests a connection for communication to the device 100. Therefore, the root certificate 222 (126) is stored in the client 200 prior to initiation of communication between the device 100 and the client 200. Furthermore, the disclosed embodiment provides that the device 100 creates the second certificate 128, which designates the root certificate 222 (126) as a certificate authority at a higher level and which is signed with the private key of the root certificate 222 (126), when the client 200 requests the device 100 for a connection for communication therebetween (see, for example, paragraph [0028] on pages 11 and 12 of the specification). Accordingly, the disclosed embodiment provides that the root certificate 222 (126) is installed in the client 200 prior to an initiation of communication between the client 200 and device 100, and then, after the client 200 requests a connection for communication to the device 100, the device 100 creates and sends the second certificate 128 to the client 200.

The above-described exemplary embodiment provides an advantageous aspect of enabling the device 100 and the client 200 to securely communicate with each other through the network 300, without requiring either the device 100 or the client 200 to purchase an electronic certificate from an authority outside the network, such as a certificate authority (CA). This is achieved because the root certificate 126 stored in the first storage device 118 of the device 100 is also stored in the second storage device 214 of the client 200, prior to an initiation of communication between the device 100 and client 200. After the client 200 requests a connection for communication to the device 100 and receives the second certificate 128 from the device 100, the verifier of the client 200 can then verify the signature of the received second certificate 128 with the root certificate 222 (126) that is stored in the second storage device 214 of the client 200. Consequently, the client 200 does not require a certificate issued by a third-party CA or a CA outside the network to verify the second certificate 128 received from the device 100.

Independent claims 1, 7, 17 and 25 recite various features of the above-described exemplary embodiment.

(1) Independent Claims 1 and 7

Claim 1 recites a communication system in which a device and a client communicate data with each other through a network.

Claim 1 recites that the device comprises a first storage device which stores a root certificate including a public key paired with a private key, and that the root certificate is signed with the private key. Claim 1 recites that the device also comprises a certificate creator which creates, when a connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key. In addition, claim 1 recites that the device comprises a communication device which transmits the second certificate, which is created by the certificate creator and signed with the private key, to the client.

Claim 1 recites that the client comprises a second storage device which has stored therein, before the connection for communication is requested to the device, the root certificate stored in the first storage device. Further, claim 1 recites that the

client comprises a verifier which verifies the signature of the second certificate received from the device with the root certificate stored in the second storage device.

Claim 7 recites a method in which the device and client perform steps corresponding to the constituent elements of the communication system of claim 1. In particular, claim 7 recites that the client installs the root certificate which is held in the device and which includes the public key, prior to the client requesting a connection for communication to the device. In addition, claim 7 recites that the device creates, when a connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key when data is sent to the client.

The Office alleged that the Smetters discloses all the recited features of claims 1 and 7, except for the recited feature that the second certificate is signed with the private key and designates the root certificate as a certificate authority at a higher level. The Office applied Benson in an attempt to teach this feature. Applicant respectfully submits that Smetters and Benson do not disclose or suggest all the recited features of claims 1 and 7 for the following reasons.

Smetters discloses a system 10 for creating a shared resource space 20 containing resources 22, 24 to be shared among a first device 12(1) and a second device 12(2) (see Figures 1 and 3). The first device 12(1), which has access to the resources 22, 24, generates a root key pair to be used for authentication and encryption when providing the device 12(2) with access to the shared space 20 (see paragraph [0025], step 100 in Figure 2, and step 120 in Figure 4). In order to share access to the space 20, the first device 12(1) generates a root certificate 30 for the space 20 and digitally signs the root certificate 30 (see paragraph [0025], step 100 in Figure 2, and step 130 in Figure 4).

Then, the first device 12(1) sends an invitation message to the second device 12(2) and establishes a secure communication channel with the second device 12(2) by sending a range-limited signal including a public key used to secure the communication between the devices 12(1), 12(2) (see paragraphs [0028]-[0030], and steps 200 and 300 in Figure 2). Smetters discloses that the second device 12(2) then decides whether to use a particular public key (e.g., the public key included in the range-limited signal from the first device 12(1) or a public key generated by the

second device 12(2) to communicate with the first device 12(1) (see paragraph [0032] and step 510 in Figure 6). If the second device 12(2) decides to use a particular public key, the second device 12(2) transmits this public key to the first device 12(1) (see paragraph [0032] and step 520 in Figure 6). On the other hand, if the second device 12(2) decides to use a public key generated by the first device 12(1), the first device 12(1) generates a pair of a public key and a private key, and sends the private key of the generated key pair to the second device 12(2) (see paragraph [0033], and steps 530 and 540 in Figure 6).

To provide the second device 12(2) with access to the shared space 20, Smetters discloses that the first device 12(1) then creates a second certificate 40 using either the public key sent from the second device 12(2) or the public key of the key pair generated by the first device 12(1). The second certificate 40 designates the second device 12(2) as a member of the shared space 20 and is equivalent to the root certificate 30 (see paragraphs [0031] and [0034], step 500 in Figure 2, and step 550 in Figure 6).

Then, the first device 12(1) sends both the root certificate 30 and the second certificate 40 to the second device 12(2), and then, the second device 12(2) stores the received root certificate 30 and second certificate 40 in a memory thereof (see paragraph [0035] and step 600 in Figure 2). The root certificate 30 and the second certificate 40 stored in the second device 12(2) form a "certificate chain", which the second device 12(2) uses to prove to other devices 12(3) that the second device 12(2) is an authorized member of the shared space 20 (see paragraph [0035]).

Smetters discloses that the first device 12(1) sends both the root certificate 30 and the second certificate 40 to the second device 12(2) at the same time, as the "certificate chain." In particular, Smetters discloses that, after the second device 12(2) has accepted the invitation from the first device 12(1), the first device 12(1) creates the second certificate 40 and then sends "both the root certificate 30 and the second laptop member certificate 40 to the [second device] 12(2)" (see paragraph [0035]) (emphasis added).

Accordingly, since the first device 12(1) sends both the root certificate 30 and the second certificate 40 to the second device at the same time after the second

certificate 40 is created, Smetters does not disclose or suggest the second storage device of the client, or the certificate creator of the device, as recited in claim 1.

In particular, Smetters does not disclose or suggest that the second device 12(2) stores the root certificate 30 before the second device 12(2) responds to the invitation from the first device 12(1) has accepted the invitation from the first device 12(1) and . On the contrary, Smetters discloses that the second device 12(2) stores the root certificate 30 and the second certificate 40, which are received at the same time as a "certificate chain," after the first device 12(1) has sent the invitation message to the second device 12(2) and the second device 12(2) has responded affirmatively to the invitation (see paragraphs [0031] and [0035]).

Accordingly, Smetters does not disclose or suggest a client comprising a second storage device which has stored therein, before the connection for communication is requested to the device, the root certificate stored in the first storage device of the device, as recited in claim 1.

Similarly, Applicant respectfully submits that Smetters does not disclose or suggest that the client installs the root certificate which is held in the device and which includes the public key, prior to the client requesting a connection for communication to the device, as recited in claim 7.

Furthermore, Applicant respectfully submits that Smetters does not disclose or suggest the certificate creator of the device, as recited in claim 1. As described above, Smetters discloses that the first device 12(1) sends an invitation message to the second device 12(2), and then generates and sends the second certificate 40, together with the root certificate 30, to the second device 12(2) if the second device 12(2) responds affirmatively to the first device's 12(1) invitation.

Claim 1 recites that the certificate creator of the device creates the second certificate, when a connection for communication is requested by the client. In contrast to claim 1, Smetters discloses that the first device 12(1) sends the invitation message to the second device 12(2) to request communication with the second device 12(2). Accordingly, Smetters does not disclose or suggest that the first device 12(1) creates the second certificate 40 when a connection for communication is requested by the second device 12(2), because the second device 12(2) does not request communication from the first device 12(1). On the contrary, the first device

12(1) requests communication from the second device 12(2) in the form of the invitation message.

Therefore, Applicant respectfully submits that Smetters does not disclose or suggest a device comprising a certificate authority which creates, when a connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key, as recited in claim 1.

Similarly, Applicant respectfully submits that Smetters does not disclose or suggest that the device creates, when a connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key when data is sent to the client, as recited in claim 7.

Furthermore, Applicant respectfully submits that Smetters clearly does not disclose or suggest the recited order in which the root certificate is stored in the client before the connection for communication is requested to the device by the client, and the certificate creator of the device creates the second certificate when the connection for communication is requested by the client, as recited in claims 1 and 7.

On the contrary, as demonstrated above, Smetters discloses the opposite configuration, in that the second device 12(2) receives both the root certificate 30 and the second certificate 40 at the same time, stores the simultaneously received certificates 30 and 40 together as a "certificate chain."

Accordingly, for at least the foregoing reasons, Applicant respectfully submits that Smetters does not disclose or suggest the certificate creator of the device and the second storage device of the client, as recited in claim 1, in addition to the corresponding operations recited in the method of claim 7. Benson also does not disclose or suggest these features of claims 1 and 7.

As noted above, the Office acknowledged that the Smetters does not disclose that the second certificate 40 is signed with a private key. On the contrary, Smetters discloses the opposite technique, in which the second certificate 40 is signed with a public key.

In particular, Smetters discloses that the second certificate 40 sent from the first device 12(1) to the second device 12(2) is signed with the public key that is transmitted from the second device 12(2) to the first device 12(1), or with the public key that is generated by the first device 12(1) (see paragraphs [0032], [0033] and [0041]). In the case where the second certificate 40 is created by using the public key generated by the first device 12(1), the first device 12(1) sends the corresponding private key to the second device 12(2), because the second device 12(2) requires the private key to access the second certificate 40.

The Office applied Benson in attempt to cure the deficiencies of Smetters for failing to disclose or suggest that the second certificate 40 is signed with a private key.

In the December 11, 2007 final Office Action and Advisory Action, the Office alleged that Column 2, lines 62-65 and Column 9, lines 46-47 of Benson disclose a second certificate signed with a private key. Specifically, in the Advisory Action, the Office asserted that "Benson explicitly discloses that descendant certificates are signed by a certificate authority's private key which is facilitated by way of the root certificate" (emphasis added, see lines 5-6 of Examiner's response in the continuation sheet of the Advisory Action). This assertion is not supportable.

Benson discloses a software protection system in which a challenge means accesses a trusted root certificate. Benson discloses that a root certificate is used to authenticate a descendent certificate, which holds a public key of a trusted source. The descendent certificate is reached from the root certificate via a certificate path (see Column 2, lines 62-65 and Column 9, lines 46-55).

However, Benson discloses that "root certificates are signed using the certificate authority's private key" (see Column 2, lines 62-63) (emphasis added). Benson does not disclose or suggest that the descendent certificates are signed with a private key of the certificate authority (CA), particularly a private key included in the root certificate and used to sign the root certificate, as recited in claims 1 and 7.

Claims 1 and 7 recite that the second certificate designates the root certificate as a certificate authority at a higher level. Accordingly, the second certificate recited in claims 1 and 7 corresponds to the "descendent certificate" of Benson.

However, Benson does not disclose or suggest that the descendent certificate is signed with a private key of the CA or a private key included in the root certificate. Instead, Benson discloses that the descendent certificate is reached (or validated) from the root certificate via a certification path, and that the descendent certificate holds a public key of a trusted source.

There is no support, either explicit or implicit, in Benson to support the Office's assertion that the descendant certificate is signed by a private key included in the root certificate and used to sign the root certificate, as recited in claims 1 and 7.

Accordingly, for at least the foregoing reasons, Applicant respectfully submits that Smetters and Benson, either individually or in combination, do not disclose or suggest all the recited features of claims 1 and 7.

Therefore, Applicant respectfully submits that claims 1 and 7 are patentable over Smetters and Benson, since Smetters and Benson, either individually or in combination, fail to disclose or suggest all the recited features of claims 1 and 7.

(2) Dependent Claims of Claims 1 and 7

In addition to the patentability of independent claims 1 and 7, Applicant respectively submits that dependent claims 8 and 20, and 22-24 of claims 1 and 7 recite further distinguishing features over Smetters and Benson.

Claim 20 recites that the root certificate stored in the first storage device is stored in the second storage device prior to the transmission of the second certificate from the communication device. Claim 23 recites that, in the method of claim 7, the device sends the second certificate to the client after the root certificate is installed in the client.

As described above, Smetters discloses that after the second device 12(2) has accepted the invitation from the first device 12(1), the first device 12(1) creates the second certificate 40 and then sends "both the root certificate 30 and the second laptop member certificate 40 to the [second device] 12(2)" (see paragraph [0035]) (emphasis added). Accordingly, since the first device 12(1) sends both the root certificate 30 and the second certificate 40 to the second device at the same time after the second certificate 40 is created, Smetters does not disclose or suggest the

above-described features of claims 20 and 23. Benson also fails to disclose or suggest the features of claims 20 and 23.

Claim 22 recites that the verifier of the client is operable to verify the signature of the second certificate by decrypting the public key of the root certificate stored in the second storage device to obtain a first hash value, calculating a second hash value of the second certificate received from the device, and comparing the first and second hash values to determine if they are equal to each other.

The Office asserted that the features recited in claim 22 are disclosed in paragraphs [0041] and [0042] of Smetters. This assertion is not supportable. Paragraphs [0041] and [0042] of Smetters do not disclose or suggest the calculation of the first and second hash values and the subsequent comparison of the first and second hash values, as recited in claim 22.

Claim 8 recites that the device further holds at least one intermediate certificate for one or more certificate authorities existing in a hierarchical order up to a root certificate authority. In addition, claim 8 recites that the client installs the at least one intermediate certificate in addition to the root certificate, and the device sends the second certificate to the client. Further, claim 8 recites that the client verifies the signature of the second certificate received from the device with the at least one intermediate certificate installed therein, and verifies the signature of the at least one intermediate certificate received from the device with the root certificate installed therein.

Claim 8 was rejected as being unpatentable over the combination of Smetters and Benson. In particular, the Office alleged that the features recited in claim 8 are disclosed by Smetters. Applicant respectfully submits that the Office has inconsistently interpreted the disclosure of Smetters in rejecting claim 8.

Smetters discloses that once the second device 12(2) has received both the root certificate 30 and the second certificate 40, the second device 12(2) may then give access to the shared space 20 to a third device 12(3). In effect, the second device 12(2) grants the third device 12(3) the access to the shared space 20 that it was granted by the first device 12(1) (see paragraph [0044]). After sending an invitation message and establishing a secure communication channel with the third device 12(3), the second device 12(3) creates a third certificate 50 for the third

device 12(3), and sends the "certificate chain" to the third device 12(3). Here, the "certificate chain" includes the root certificate 30 created by the first device 12(1), the second certificate 40 created by the first device 12(1) for the second device 12(2), and the third certificate 50 created by the second device 12(2) for the third device 12(3) (see paragraph [0045] and Figure 7).

By depending from claim 7, claim 8 further defines the limitations recited in claim 7. Claim 7 recites that the device creates and sends the second certificate to the client. Therefore, the "device" of claims 7 and 8 can only be considered to correspond to the first device 12(1) of Smetters, and the "client" of claims 7 and 8 can only be considered to correspond to the second device 12(2) of Smetters.

The second device 12(2) of Smetters cannot correspond to the "device" of claims 7 and 8, because the second device 12(2) does not create the second certificate 40, in contrast to claim 7. The second device 12(2) creates the third certificate 50, which is the lowest certificate in the hierarchy of the "certificate chain" received by the third device 12(3). On the other hand, the second certificate recited in claim 8 is the lowest certificate in the hierarchy of a certificate chain, because the client is recited in claim 8 as verifying the signature of the second certificate with the at least one intermediate certificate installed in the client, and verifying the signature of the at least one intermediate certificate with the root certificate installed in the client. Thus, the at least one intermediate certificate of claim 8 can only be considered to correspond to the second certificate 40 of Smetters, and the second certificate of claim 8 can only be considered to correspond to the third certificate 50 of Smetters.

However, in contrast to claim 8, the first device 12(1) of Smetters, which can only be considered to correspond to the device of claim 8, does not send the third certificate 50 to the second device 12(2). Instead, as described above, the second device 12(2), independent of the first device 12(1), creates and sends the third certificate 50 (corresponding to the second certificate of claim 8) to the third device 12(3). Accordingly, Smetters does not disclose or suggest the step of the device sending the second certificate to the client, as recited in claim 8.

Furthermore, Smetters discloses that the third device 12(3) verifies the third certificate 50 by using the second certificate 40. Accordingly, Smetters also does not

disclose or suggest that the client (second device 12(2)) verifies the signature of the second certificate (third certificate 50) received from the device (first device 12(1)) with the at least one intermediate certificate (second certificate 40) installed therein, and verifies the signature of the at least one intermediate certificate (second certificate 40) received from the device (first device 12(1)) with the root certificate (root certificate 30) installed therein, as recited in claim 8.

Claim 24, which depends from claim 8, recites that the client installs the at least one intermediate certificate prior to receiving the second certificate from the device. Smetters does not disclose or suggest this feature for at least two reasons. First, the second device 12(2) (client of claim 8) does not receive the third certificate 50 (corresponding to the second certificate of claim 8). Second, even if the second device 12(2) did receive the third certificate 50, the third certificate 50 is sent at the same time with the first and second certificates 30, 40 as a "certificate chain".

Accordingly, Applicant submits that Smetters does not disclose or suggest the features of claims 8 and 24. Benson also fails to disclose or suggest the features of claims 8 and 24.

For at least the foregoing reasons, Applicant submits that Smetters and Benson, either individually or in combination, do not disclose or suggest the features of claims 8, 20 and 22-24.

Therefore, in addition to the patentability of claims 1 and 7 demonstrated above, Applicant respectfully submits that claims 8, 20 and 22-24 recite further distinguishing features over Smetters and Benson.

(3) Independent Claims 17 and 25

Claims 17 and 25 were identified in paragraph 8 on page 3 as being rejected over the combination of Smetters and Benson. However, the Office Action does not include a discussion of the features of claims 17 and 25, or the Office's application of Smetters and Benson with respect to the features of claims 17 and 25.

Nevertheless, Applicant respectfully submits that claims 17 and 25 are patentable over Smetters and Benson for at least the following reasons.

Claims 17 and 25 each recite a device to be used in a communication system in which a device and a client communicate with each other through a network.

Claims 17 and 25 each recite that the device comprises a second storage device which stores a root certificate signed with the private key. Claims 17 and 25 also each recite that the device comprises a certificate creator which creates, when a connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level.

In addition, claims 17 and 25 each recite that the device comprises an interface which sends the information as well as the root certificate including the public key to the client through the network before the connection for communication is requested to the device, and sends, after the root certificate is installed in the client, the second certificate to the client for verification of the information sent from the device.

As described above, Smetters discloses that after the first device 12(1) initiates communication with the second device 12(2) and creates the second certificate 40 for the second device 12(2), the first device 12(1) sends both the root certificate 30 and the second certificate 40 at the same time to the second device 12(2) as a "certificate chain" (see paragraph [0035]). Accordingly, in contrast to claims and 17 and 25, Smetters does not disclose or suggest a device comprising an interface which sends the information as well as the root certificate including the public key to the client through the network before the connection for communication is requested to the device, and sends, after the root certificate is installed in the client, the second certificate to the client for verification of the information sent from the device. Benson also fails to disclose or suggest these features of claims 17 and 25.

Furthermore, as described above, Smetters discloses that the first device 12(1) initiates communication with the second device 12(2) by sending an invitation to the second device 12(2) to access the space 20, and then generates and sends the second certificate 40, together with the root certificate 30, to the second device 12(2) if the second device 12(2) responds affirmatively to the first device's 12(1) invitation.

Therefore, Applicant respectfully submits that Smetters does not disclose or suggest a device comprising a certificate creator which creates, when a connection for communication is requested by the client, a second certificate designating the

root certificate as a certificate authority at a higher level, as recited in claims 17 and 25. Benson also fails to disclose or suggest these features of claims 17 and 25.

In addition, claim 17 recites that the second certificate created by the device is signed with the private key. As demonstrated above, Benson does not disclose or suggest that a descendant certificate is signed with a private key, instead disclosing that a root certificate is signed with the certificate authority's private key. Therefore, Applicant respectfully submits that Benson also fails to disclose or suggest this feature of claim 17.

Accordingly, for at least the foregoing reasons, Applicant respectfully submits that claims 17 and 25 are also patentable over Smetters and Benson, since Smetters and Benson, either individually or in combination, do not disclose or suggest all the recited features of claims 17 and 25.

B. Dependent claims 2 and 3 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Smetters in view of Benson and further in view of Debry (U.S. 6,918,042). Dependent claims 9, 11, 18-19, 26 and 27 were rejected under 35 U.S.C. § 103(a) as unpatentable Smetters in view of Benson and Debry and further in view of Slick et al. (U.S. Patent Publication No. 2004/01109568, hereinafter "Slick"). Further, dependent claim 6 was rejected under 35 U.S.C. § 103(a) as unpatentable over Smetters and Benson and further in view of Vogel et al. (U.S. Patent No. 6,816,900, hereinafter "Vogel").

Without acquiescing to the Office's application of Debry, Slick and Vogel to the features of dependent claims 2, 3, 6, 9, 11, 18, 19, 26, 27, Applicant respectfully submits that Debry, Slick and Vogel, either individually or in combination, do not cure the deficiencies of Smetters and Benson for failing to disclose or suggest all the recited features of independent claims 1, 7, 17 and 25.

Therefore, no obvious combination of Smetters, Benson, Debry, Slick and Vogel would result in the subject matter of independent claims 1, 7, 17 and 25, as well as claims 2-6, 8-12, 18, 19, 20-24, 26 and 27 which depend therefrom, since these references, either individually or in combination, fail to disclose or suggest all the recited features of at least independent claims 1, 7, 17 and 25.

The foregoing explanation of the patentability of independent claims 1, 7, 13, 17 and 25 is sufficiently clear such that it is believed that separately arguing the patentability of the dependent claims whose rejections were not traversed above is unnecessary at this time. However, Applicant reserves the right to do so if it becomes appropriate.

III. Conclusion

In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is clearly in condition for allowance. Accordingly, a favorable examination and consideration of the instant application are respectfully requested.

If, after reviewing this Amendment, the Examiner believes there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: June 11, 2008

By: /Jonathan R. Bowser/
Jonathan R. Bowser
Registration No. 54574

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620